UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

EVELYN NELSON, individually, as natural parent and next friend of J.N. I and J.N. II, minors, and on behalf of all others similarly situated, *Plaintiff,* v. CONNEXIN SOFTWARE INC. d/b/a OFFICE PRACTICUM, *Defendant*.	**Case No. 2:22-cv-4676** **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Evelyn Nelson ("Plaintiff"), individually and on behalf of a class of similarly situated persons, brings this Class Action Complaint and alleges the following against defendant Connexin Software, Inc. d/b/a Office Practicum ("Connexin" or "Defendant"), based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Connexin for its failure to properly secure and safeguard protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), and other personally identifiable information ("PII"). The PII included without limitation: names of children and parents; dates of birth; and Social Security numbers. The PHI included without limitation: medical information, including diagnoses; provider's names; medical record numbers; health insurance information; and treatment information.

2. Connexin failed to comply with industry standards to protect information systems that contain that PII and PHI, and failed to provide timely, accurate, and adequate notice to

Plaintiff and other Class Members that their PII and PHI had been compromised. Plaintiff seeks, among other things, orders requiring Connexin to fully and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the disclosure (the "Data Breach") in the future.

3. On November 14, 2022, Connexin reported to the Montana Attorney General a data breach affecting 17,172 individuals in that state alone. The form notice letter Connexin submitted with that report discloses the following:

> On September 13, 2022, we learned that an unauthorized party was able to access an offline set of patient data used for data conversion and troubleshooting. Some of that data was *removed* by the unauthorized party.

Ex. 1 (emphasis added). The letter is ambiguous as to whether the "unauthorized party" merely copied the patient data, erased it, or both.

4. On or around November 17, 2022, Connexin reported to the Texas Attorney General that the incident affected 213,638 individuals in that state alone.

5. A notice available only on Connexin's websites identifies dozens of pediatric practices whose patients were affected by the data breach. *See* Ex. 2.[1]

6. As a result of Connexin's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PHI and PII is now in the hands of criminals. Plaintiff and Class Members face a substantial increased risk of identity theft, both currently and for the indefinite future. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves and their children due to Connexin's failures.

[1]Available at https://www.officepracticum.com/substitute-notice/ (last accessed Nov. 21, 2022).

7. The harm is greater with respect to the child victims. As one expert recently observed, hackers "target pediatric records to carry out fake loans with victims potentially none the wiser for years."[2]

8. Plaintiff seeks to remedy these harms individually and on behalf of all other similarly situated individuals whose PII and/or PHI were stolen in the Data Breach. Plaintiff seeks remedies including compensation for time spent responding to the Data Breach and other types of harm, free credit monitoring and identity theft insurance, and injunctive relief including substantial improvements to Connexin's data security systems.

PARTIES

9. Plaintiff Evelyn Nelson resides in Lawrence, Kansas. Ms. Nelson's children have been patients at Children's Mercy – Pediatric Partners, Inc., over the course of approximately three years. Children's Mercy – Pediatric Partners, Inc. is identified on Connexin's website as one of the practices whose patients were victimized by the Data Breach. Ex. 2, at 3.

10. Defendant Connexin Software, Inc. d/b/a Office Practicum is a Maryland corporation, with its principal office in Fort Washington, Pennsylvania.

11. Connexin refers to itself as "[t]he industry leader in pediatric-specific Health Information Technology Solutions" and claims that it "provides pediatric-specific health information technology solutions for independent pediatric practices."[3] Connexin claims to serve

[2] Michael Novinson, "Hospital CISO on Why Hackers Pursue Research, Pediatric Data", Bank Info Security, Nov. 15, 2022 (available at https://www.bankinfosecurity.com/hospital-ciso-on-hackers-pursue-research-pediatric-data-a-20461) (last accessed Nov. 21, 2022).

[3] *See* Office Practicum LinkedIn page (available at https://www.linkedin.com/company/officepracticum/about/) (last accessed Nov. 21, 2022).

over 9,000 pediatricians across 49 states.[4] Due to the nature of these services, Connexin acquires and electronically stores patient PII and PHI.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Connexin is a citizen of a state different from that of at least one Class Member.

13. This Court has personal jurisdiction over Connexin because it is a resident of the Commonwealth of Pennsylvania.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because Connexin transacts business and may be found in this District.

FACTUAL ALLEGATIONS

The Data Breach

15. Connexin provides information technology services for thousands of pediatricians nationwide. As a vendor to healthcare providers, Connexin is required to ensure that PII and PHI are not disclosed or disseminated to unauthorized third parties without their patients' express written consent.

[4] *See* "Office Practicum to Offer the Market's First 'Whole Child' Digital Healthcare Platform" (available at https://www.prnewswire.com/news-releases/office-practicum-to-offer-the-markets-first-whole-child-digital-healthcare-platform-301491091.html) (last accessed Nov. 21, 2022).

16. On November 14, 2022, Connexin reported a hacking incident to the Montana Attorney General that compromised the data of 17,172 individuals in that state alone.

17. On or around November 17, 2022, Connexin reported to the Texas Attorney General that the incident affected 213,638 individuals in that state alone.

18. The form notice letter that Connexin submitted to the Montana Attorney General disclosed the following:

> The patient information may have included: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider).

See Ex. 1.

19. Connexin's disclosures are otherwise deficient. They do not include basic details concerning the Data Breach, including, but not limited to, why PII and PHI were stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the data was encrypted or otherwise protected, and whether Connexin knows if the data has been further disseminated.

20. Connexin has not nearly disclosed all the details of the Data Breach and its investigation. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, Connexin has taken to secure the PII and PHI still in its possession. Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses the harm to Plaintiff's and Class

Members' interests, and ensure that Connexin has proper measures in place to prevent similar incidents from occurring in the future.

Connexin's Privacy Policies

21. HIPAA requires that Connexin maintain strict privacy practices. Connexin's Privacy Policy notes that "[p]rotecting the privacy of the very young is especially important."[5] Connexin also acknowledges that "some healthcare providers and patients may be concerned about medical privacies [sic] when using EHRs [electronic health records]. Common concerns include lost information due to a natural disaster and cyber hacks."[6] *See also* "Pediatric EHR Software Designed By Pediatricians For Pediatricians" ("Data privacy is one of the biggest areas of concern these days.").[7]

22. Connexin's website includes multiple specific claims about the security of its services. One page claims that its services "gives parents 24/7 access to their child's health records, while protecting the patient's privacy," and include "features help them ensure that the patient's safety and privacy remain protected."[8] *See also* "Pediatric-Specific EHR" ("Adolescent-Care Functionality" "maintains adolescent privacy and confidentiality")[9]; "21st

[5] *See* Privacy Policy (available at https://www.officepracticum.com/privacy-policy/) (last accessed Nov. 21, 2022).

[6] *See* "6 Common Challenges In EHR Implementation" (available at https://www.officepracticum.com/blog/6-common-challenges-in-ehr-implementation/) (last accessed Nov. 21, 2022).

[7] Available at https://www.officepracticum.com/pediatric-ehr-software/ (last accessed Nov. 21, 2022).

[8] *See* OP Patient Portal (available at https://www.officepracticum.com/resources/mlw/complete-childrens-health-portal) (last accessed Nov. 21, 2022).

[9] Available at https://www.officepracticum.com/pediatric-specific-EHR-18 (last accessed Nov. 21, 2022)

Century CURES Act" ("Having adolescent privacy settings, our EHR allows you to granularly protect sensitive information.").[10]

The Healthcare Sector is a Primary Target for Data Breaches

23. Connexin was on notice that companies in the healthcare industry are susceptible targets for data breaches.

24. Connexin was also on notice that the Federal Bureau of Investigation has been concerned about data security in the healthcare industry. On April 8, 2014, the FBI's Cyber Division issued a Private Industry Notification to companies within the healthcare sector, stating that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and pointed out that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise." The same warning specifically noted that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or PII."[11]

[10] Available at https://www.officepracticum.com/pediatric-solutions-cures-act) (last accessed Nov. 21, 2022).

[11] (U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain (Apr. 8, 2014), FBI Cyber Division Private Industry Notification (available at https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf) (last accessed Oct. 6, 2022).

25. The number of reported North American data breaches increased by over 50 percent in 2021, from 1,080 in 2020[12], to 1,638 in 2021.[13] As a recent report reflects, "[h]ealthcare has increasingly become a target of run-of-the-mill hacking attacks and the more impactful ransomware campaigns."[14]

26. At the end of 2018, the healthcare sector ranked second in the number of data breaches among measured sectors, and had the highest rate of exposure for each breach.[15] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[16] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy.[17]

---

[12] *See* Verizon 2021 Data Breach Investigations Report, at 97, https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf (last accessed Oct. 6, 2022).

[13] *See* Verizon 2022 Data Breach Investigations Report, at 83 (available at https://www.verizon.com/ business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf) (last accessed Oct. 6, 2022).

[14] *Id.* at 62.

[15] *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center (available at https://www.idtheftcenter.org/2018-data-breaches) (last accessed Oct. 6, 2022).

[16] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) (available at https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/) (last accessed Oct. 6, 2022).

[17] *Id.*

27. Healthcare related breaches have persisted because criminals see electronic patient data as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the previous 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[18] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[19]

28. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[20]

29. As a major vendor to healthcare providers, Connexin knew, or should have known, the importance of safeguarding the patients' PII and PHI entrusted to it and of the

---

[18] *2019 HIMSS Cybersecurity Survey* (available at https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf) (last accessed Oct. 6, 2022).

[19] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Apr. 4, 2019 (available at https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks) (last accessed Oct. 6, 2022).

[20] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019) (available at https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals) (last visited Oct. 6, 2022).

foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on Connexin's customers' patients because of a breach. Connexin failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Connexin Stores Plaintiff's and Class Members' PII and PHI

30. Connexin obtains and stores a massive amount of its customers' patients' PII and PHI. As a condition of engaging in health services, Connexin's customers require that patients entrust it with highly confidential PII and PHI.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Connexin assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from disclosure.

32. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and, as current and former patients of Connexin's customers, they rely on Connexin to keep this information confidential and securely maintained, and to make only authorized disclosures of this information.

PII and PHI are Valuable and Subject to Unauthorized Disclosure

33. Connexin was aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

34. PII and PHI are valuable commodities to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[21] Indeed, a robust illegal market exists in which criminals

[21] Federal Trade Commission, What To Know About Identity Theft (available at https://consumer.ftc.gov/articles/what-know-about-identity-theft) (last accessed Oct. 6, 2022).

openly post stolen PII and PHI on multiple underground websites, commonly referred to as the "dark web." PHI can sell for as much as $363 on the dark web, according to the Infosec Institute.[22]

35. PHI is particularly valuable because criminals can use it to target victims with frauds and swindles that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

36. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's PHI is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[23]

37. The ramifications of Connexin's failure to keep its customers' patients' PII and PHI secure are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for months or even years thereafter.

---

[22] Center for Internet Security, *Data Breaches: In the Healthcare Sector* (available at https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/) (last accessed Oct. 6, 2022).

[23] Michael Ollove, The Rise of Medical Identity Theft in Healthcare, Kaiser Health News (Feb. 7, 2014) (available at https://khn.org/news/rise-of-indentity-theft/) (last accessed Oct. 6, 2022).

38. Further, criminals often trade stolen PII and PHI for years following a breach. Cybercriminals can post stolen PII and PHI on the internet, thereby making such information publicly available.

39. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[24] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[25]

40. Here, not only was PHI compromised, but also patient Social Security numbers. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[26] This time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

41. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement

[24] *See* Medical ID Theft Checklist (available at https://www.identityforce.com/blog/medical-id-theft-checklist-2) (last accessed Oct. 6, 2022).

[25] Experian, The Potential Damages and Consequences of Medical Identityy Theft and Healthcare Data Breaches (available at https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf) (last accessed Oct. 6, 2022).

[26] *Identity Theft and Your Social Security Number*, Social Security Administration (available at http://www.ssa.gov/pubs/EN-05-10064.pdf) (last accessed Oct. 6, 2022).

notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

42. Changing or cancelling a stolen Social Security number is extremely difficult. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

43. Even then, a new Social Security number may not be effective. According to the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[27]

44. Connexin knew, or should have known, the importance of safeguarding its customers' patients' PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Connexin's customers' patients because of a breach. Connexin failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

The Data Breach Exposed Plaintiff and Class Members to Identity Theft and Out-of-Pocket Losses

45. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of their rights. They are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

[27] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015) (available at http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft) (last visited Oct. 6, 2022).

46. Despite all the publicly available knowledge of the disclosure of PII and PHI, Connexin's policies and practices with respect to maintaining the security of its customers' patients' PII and PHI were reckless, or at the very least, negligent.

47. In virtually all contexts, the expenditure of time has consistently been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be compensated for the time they have expended because of Connexin's misfeasance.

48. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[28]

49. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer financial loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their PII and PHI;

b. identity theft and fraud resulting from the theft of their PII and PHI;

c. costs associated with the detection and prevention of identity theft;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

[28] 2014 LexisNexis True Cost of Fraud Study (available at https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf) (last accessed Oct. 6, 2022).

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

g. the continued imminent injury flowing from potential fraud and identify theft posed by their PII and PHI being in the possession of one or more unauthorized third parties.

Connexin's Lax Security Violates HIPAA

50. Connexin had a non-delegable duty to ensure that all PHI it collected and stored was secure.

51. Connexin is bound by HIPAA (*see* 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

52. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. See 45 C.F.R. § 160.103.

53. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

54. HIPAA requires that Connexin implement appropriate safeguards for this information.

55. Despite these requirements, Connexin failed to comply with its duties under HIPAA and its own Privacy Practices. In particular, Connexin failed to:

a. maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. adequately protect Plaintiff's and Class Members' PHI;

c. ensure the confidentiality and integrity of electronic PHI created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. ensure compliance with the electronic PHI security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. train all members of its workforce effectively on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their responsibilities and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b)

56. Connexin failed to comply with its duties under HIPAA despite being aware of the risks associated with unauthorized access to Plaintiff's and Class Members' PHI.

Connexin Violated FTC Guidelines

57. The Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, prohibited Connexin from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' PII is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

58. The FTC has promulgated several guides for businesses that reflect the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[29]

59. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established data security guidelines for businesses.[30] The guidelines

[29] Federal Trade Commission, Start With Security: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last accessed Oct. 6, 2022).

[30] Federal Trade Commission, Protecting Personal Information: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last accessed Oct. 6, 2022).

reflect that businesses should protect the PII that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

60. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to confidential data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[31]

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. Connexin failed to properly implement basic data security practices. Connexin's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

63. Connexin was at all times fully aware of its obligation to protect the PII and PHI of its customers' patients because of their positions as healthcare providers. Connexin was also aware of the significant repercussions that would result from its failure to do so.

---

[31] FTC, *Start With Security*, *supra*.

CLASS ACTION ALLEGATIONS

64. Pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure, Plaintiff seeks certification of a Class as defined below:

> All persons in the United States whose PII and/or PHI was exposed by the Data Breach that was disclosed by Connexin on or around November 14, 2022.

65. Excluded from the Class are Connexin, any entity in which Connexin has a controlling interest, and Connexin's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

66. Plaintiff reserves the right to modify or amend the definition of the proposed Class as additional information becomes available to Plaintiff.

67. **Numerosity:** The Class Members are so numerous that individual joinder of all Class Members is impracticable. In its report to the Texas Attorney General, Connexin attested that the Data Breach affected at least 213,000 patients in that state alone. All Class Members' names and addresses are available from Connexin's and/or its customers' records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

68. **Commonality:** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Connexin had a duty to protect the PII and PHI of Class Members;

b. Whether Connexin was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI;

c. Whether Connexin had duties not to disclose the PII and PHI of Class Members to unauthorized third parties;

d. Whether Connexin took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII and PHI;

e. Whether Connexin failed to adequately safeguard the PII and PHI of Class Members;

f. Whether Connexin failed to implement and maintain reasonable security policies and practices appropriate to the nature and scope of the PII and PHI compromised in the Data Breach;

g. Whether Connexin adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

h. Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages because of Connexin's wrongful conduct;

a. Whether Plaintiff and Class Members are entitled to restitution because of Connexin's wrongful conduct;

b. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm they face because of the Data Breach; and

c. Whether Plaintiff and Class Members are entitled to identity theft protection for their respective lifetimes.

69. **Typicality:** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII and PHI, like that of every other Class Member, was disclosed by Connexin. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through Connexin's common misconduct. Plaintiff is advancing the same

claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. Plaintiff's claims and Class Members' claims arise from the same operative facts and are based on the same legal theories.

70. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Connexin to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's counsel are competent and experienced in litigating class actions, including extensive experience in data breach litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

71. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Connexin has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Connexin's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Connexin's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

72. **Superiority:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually

afford to litigate a complex claim against large corporations, like Connexin. Even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

73. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Connexin would necessarily gain an unconscionable advantage in non-class litigation, since Connexin would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by Class Members and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

74. The litigation of Plaintiff's claims is manageable. Connexin's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with maintenance of this lawsuit as a class action.

75. Adequate notice can be given to Class Members directly using information maintained in Connexin's and/or its customers' records.

76. Unless a class-wide injunction is issued, Connexin may continue to maintain inadequate security with respect to the PII and PHI of Class Members, Connexin may continue to

refuse to provide proper notification to Class Members regarding the Data Breach, and Connexin may continue to act unlawfully as set forth in this Complaint.

COUNT I
NEGLIGENCE

77. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

78. As a condition of their utilizing Connexin's customers' services, patients were obligated to provide Connexin with certain PII and PHI, including their dates of birth, Social Security numbers, personal medical information, and other PII and PHI.

79. Plaintiff and the Class Members entrusted their PII and PHI to Connexin on the premise and with the understanding that Connexin would safeguard their information and not disclose that information to unauthorized third parties.

80. Connexin has full knowledge of the sensitivity of PII and PHI and the types of harm that Plaintiff and Class Members could and would suffer if PII and PHI were wrongfully disclosed.

81. Connexin knew or reasonably should have known that the failure to exercise due care in the collection, storage, and use of patients' PII and PHI involved an unreasonable risk of harm to Plaintiff and Class Members.

82. Connexin had a duty to exercise reasonable care in safeguarding, securing, and protecting Plaintiff's and Class Members' PII and PHI from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Connexin's security protocols to ensure that Plaintiff's and Class Members' information in Connexin's possession was adequately secured and protected,

and that employees tasked with maintaining such information were adequately trained as to proper measures regarding the security of patients' PII and PHI.

83. Connexin had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII and PHI.

84. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Connexin, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Connexin's duty in this regard.

85. Connexin violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI and failing to comply with relevant industry standards. Connexin's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

86. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly considering the growing number of data breaches of health care providers.

87. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Connexin knew or should have known of the inherent risks in collecting and storing Plaintiff's and Class Members' PII and PHI, the importance of providing adequate security for that information, and that Connexin had inadequate employee training and education and information technology security protocols in place to secure Plaintiff's and Class Members' PII and PHI.

88. Connexin's misconduct created a foreseeable risk of harm to Plaintiff and Class Members. Connexin's misconduct included, but was not limited to, its failure to take the steps necessary to prevent the Data Breach. Connexin's misconduct also included its decisions not to comply with industry standards for the safekeeping and disclosure of Plaintiff's and Class Members' PII and PHI.

89. Plaintiff and Class Members had no ability to protect their PII and PHI that was in Connexin's possession.

90. Connexin was in a position to protect against the harm suffered by Plaintiff and Class Members because of the Data Breach.

91. Connexin had and continues to have a duty to adequately disclose that Plaintiff's and Class Members' PII and PHI within Connexin's possession might have been compromised, how it was compromised, and precisely the types of information that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PHI by unauthorized parties.

92. Connexin has admitted that Plaintiff's and Class Members' PII and PHI was wrongfully disclosed to unauthorized parties because of the Data Breach.

93. Connexin, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII and PHI during the period in which that information was within Connexin's possession or control.

94. Connexin failed to heed industry warnings and alerts to provide adequate safeguards to protect patients' PII and PHI in the face of increased risk of theft.

95. Connexin, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PII and PHI.

96. Connexin, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

97. But for Connexin's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII and PHI would not have been compromised.

98. There is a close causal connection between Connexin's failure to implement security measures to protect the PHI of its customers' current and former patients and the harm suffered or risk of imminent harm suffered by Plaintiff and Class Members. Unauthorized parties gained access to Plaintiff's and Class Members' PII and PHI as the proximate result of Connexin's failure to exercise reasonable care in safeguarding that information by adopting, implementing, and maintaining appropriate security measures.

99. As a direct and proximate result of Connexin's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with the effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit

reports; (vii) the continued risk to their PII and PHI, which remains in Connexin's possession and is subject to further unauthorized disclosures so long as Connexin fails to undertake appropriate and adequate measures to protect that information; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Connexin's services Plaintiff and Class Members received.

100. As a direct and proximate result of Connexin's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
NEGLIGENCE PER SE

101. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

102. Pursuant to the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, Connexin had a duty to provide adequate data security practices, including in connection with its sale of its services to Plaintiff's and Class Members' pediatric practices.

103. Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1302d, et seq., Connexin had a duty to implement reasonable safeguards to protect Plaintiff's and Class Member's PII/PHI.

104. Connexin breached its duties to Plaintiff and Class Members under the FTC Act and HIPAA, among other laws, by failing to provide fair, reasonable, or adequate data security in connection with the sale and use of its services, in order to safeguard Plaintiff's and Class Members' PII/PHI.

105. Connexin's failure to comply with applicable laws and regulations constitutes negligence per se.

106. But for Connexin's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

107. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Connexin's breach of its duties. Connexin knew or should have known that it was failing to meet its duties, and that its breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII/PHI.

108. As a direct and proximate result of Connexin's negligent conduct, Plaintiff and Class Members face an increased risk of future harm.

109. As a direct and proximate result of Connexin's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
UNJUST ENRICHMENT

110. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

111. Plaintiff and Class Members have an interest, both equitable and legal, in their PHI and PII that was conferred upon, collected by, and maintained by Connexin and that was ultimately stolen in the Data Breach.

112. Connexin benefitted from the conferral upon it of Plaintiff's and Class Members' PII and PHI, and by its ability to retain and use that information. Connexin understood that it so benefitted.

113. Connexin also understood and appreciated that Plaintiffs' and Class Members' PHI and PII was private and confidential and that its value depended upon Connexin maintaining its privacy and confidentiality.

114. But for Connexin's willingness and commitment to maintain its privacy and confidentiality, that PHI and PII would not have been transferred to and entrusted with Connexin. Further, if Connexin had disclosed that its data security measures were inadequate, Connexin would not have been permitted to continue in operation by regulators and the healthcare marketplace.

115. As a result of Connexin's wrongful conduct as alleged in this Complaint (including among other things its utter failure to employ adequate data security measures, its continued maintenance and use of Plaintiff's and Class Members' PHI without having adequate data security measures, and its other conduct facilitating the theft of that PHI and PII), Connexin has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

116. Connexin's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compilation and use of Plaintiff's and Class Members' sensitive PHI and PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers.

117. Under the common law doctrine of unjust enrichment, it is inequitable for Connexin to be permitted to retain the benefits it received, and is still receiving, without justification, from the use of Plaintiff's and Class Members' PHI and PII in an unfair and unconscionable manner. Connexin's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

118. The benefit conferred upon, received, and enjoyed by Connexin was not conferred officiously or gratuitously, and it would be inequitable and unjust for Connexin to retain the benefit.

COUNT IV
INJUNCTIVE/DECLARATORY RELIEF

119. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

120. Connexin owes a duty of care to Plaintiff and Class Members requiring it to adequately secure PII and PHI.

121. Connexin still stores Plaintiff's and Class Members' PII and PHI.

122. Since the Data Breach, Connexin has announced no specific changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent similar incidents from occurring in the future.

123. Connexin has not satisfied its legal duties to Plaintiff and Class Members.

124. Actual harm has arisen in the wake of the Data Breach regarding Connexin's duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and PHI, and Connexin's failure to address the security failings that led to that exposure.

125. Plaintiff, therefore, seeks a declaration: (a) that Connexin's existing security measures do not comply with its duties of care to provide adequate security; and (b) that to comply with its duties of care, Connexin must implement and maintain reasonable security measures, including, but not limited to, the following:

a. ordering that Connexin engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Connexin's systems on a periodic basis, and ordering Connexin to promptly correct any problems or issues detected by such third-party security auditors;

b. ordering that Connexin engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Connexin audit, test, and train its security personnel regarding any new or modified procedures;

d. ordering that Connexin segment patient data by, among other things, creating firewalls and access controls so that if one area of Connexin's system is compromised, hackers cannot gain access to other portions of Connexin's systems;

e. ordering that Connexin purge, delete, and destroy in a reasonably secure manner patient data not necessary for its provision of services;

f. ordering that Connexin conduct regular computer system scanning and security checks;

g. ordering that Connexin routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Connexin to meaningfully educate its current, former, and prospective patients about the threats they face because of the loss of their PHI to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, prays for relief as follows:

a. for an Order certifying the Class as defined herein, and appointing Plaintiff and her counsel to represent the Class;

b. for equitable relief enjoining Connexin from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

c. for equitable relief compelling Connexin to use appropriate cyber security methods and policies with respect to PII and PHI collection, storage, and protection, and to disclose with specificity to Class Members the types of PII and PHI compromised;

d. for an award of damages, including actual, nominal, consequential, enhanced compensatory, and punitive damages, as allowed by law in an amount to be determined;

e. for an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. for prejudgment interest on all amounts awarded; and

g. such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: November 22, 2022

Respectfully submitted,

BAILEY GLASSER LLP

/s/ Bart D. Cohen

By: Bart D. Cohen (PA Bar No. 57606)
1622 Locust Street
Philadelphia, PA 19103
(215) 274-9420
bcohen@baileyglasser.com

Attorneys for Plaintiff and the Proposed Class

EXHIBIT 1

<<Date>> (Format: Month Day, Year)

Parent or Guardian of
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Su información personal de su hijo puede haber estado involucrada en un incidente de datos.
Si desea recibir una version de esta carta en español, por favor llame 855-532-0912.

Notice of Data Breach

To the Parent or Legal Guardian of <<Patient Name>>:

We are writing to inform you of a data security incident that occurred at Connexin Software, Inc. (Connexin) that may have affected your child's personal information. Connexin provides electronic medical records and practice management software, billing services, and business analytic tools to its physician's practice groups, including <<Covered Entity Name>>, from which your child may have received services.

What happened?

On August 26, 2022, Connexin detected a data anomaly on our internal network. We immediately launched an investigation and engaged third-party forensic experts to determine the nature and scope of the incident. On September 13, 2022, we learned that an unauthorized party was able to access an offline set of patient data used for data conversion and troubleshooting. Some of that data was removed by the unauthorized party. The live electronic record system was not accessed in this incident, and the incident did not involve <<Covered Entity Name>>'s systems, databases, or medical records system at all.

What information may have been involved?

Although we are unaware of any actual or attempted misuse of personal information because of this incident to date, we are notifying you because your child's information may have been involved.

The patient information may have included: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers);

and (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider). Please note that not all data fields may have been involved for all individuals.

As a parent, guardian, or guarantor, your information may have been impacted as well by the incident. If that is the case, you will receive a separate letter from Connexin.

What we are doing.

Data security is very important to us. As soon as we discovered the incident, we immediately took action to stop the unauthorized activity. This included a password reset of all corporate accounts and moving all patient data used for data conversion and troubleshooting into an environment with even greater security. Connexin also retained a third-party cybersecurity forensic firm to investigate the issue and is working with law enforcement to investigate the incident. In response to this incident, Connexin has enhanced its security and monitoring as well as further hardened its systems as appropriate to minimize the risk of any similar incident in the future.

In addition, Connexin has arranged to offer your child identity monitoring services for a period of one year, at no cost to you, through Kroll. You have until <<vtext 6(activation deadline)>> to activate these services, and instructions on how to activate these services are included in the enclosed Reference Guide.

What you can do.

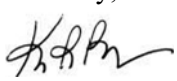
In addition to activating the complimentary identity monitoring services, the enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your child's personal information. We encourage you to carefully review credit reports and statements sent from providers as well as your insurance company to ensure that all account activity is valid; any questionable charges should be promptly reported to the provider's billing office, or for insurance statements, to your insurance company.

For more information

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, or call toll-free 855-532-0912. This call center is open from 8:00am – 5:30pm CT, Monday through Friday, excluding some U.S. holidays.

We sincerely regret and apologize that this incident occurred. Connexin takes the security of personal information seriously, and we will continue to work diligently to protect the information entrusted to us.

Sincerely,



Kraig Brown
CEO

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide any updated personal information to your health care provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Activate Kroll Identity Monitoring Services

As a safeguard, we have arranged for you to activate, at no cost to you, in online identity monitoring services provided by Kroll.

To activate this service, please visit **<<IDMonitoringURL>>** and follow the instructions for activation using Membership Number: **<< Member ID >>**

The monitoring included in the membership must be activated to be effective. You have until <<vtext 6(activation deadline)>> to activate these services. Please note that identity monitoring services may not be available for individuals who do not have an address in the United States (or its territories) and a valid Social Security number. Activating this service will not affect your credit score.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail,

or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	888-298-0045	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of the District of Columbia

You may contact the D.C. Attorney General's Office to obtain information about steps to take to avoid identity theft:

D.C. Attorney General's Office, Office of Consumer Protection, 400 6th Street, NW, Washington DC 20001, 1-202-442-9828, www.oag.dc.gov.

For Residents of Iowa

You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at:

Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowattorneygeneral.gov.

For Residents of Maryland

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, http://www.marylandattorneygeneral.gov/.

For Residents of Massachusetts

You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Residents of New Mexico

New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For Residents of New York

You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, www.ncdoj.gov.

For Residents of Oregon

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us.

For Residents of Rhode Island

You have a right to file or obtain a police report related to this incident. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Office of the Attorney General, 150 South Main Street, Providence, RI, 02903, 1-401-274-4400, www.riag.ri.gov.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Minor Identity Monitoring
Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent to you when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Fraud Consultation
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

EXHIBIT 2

Unauthorized Access to Internal Computer Network at Connexin Software, Inc.

Connexin Software, Inc. (Connexin), a provider of electronic medical records and practice management software, billing services, and business analytic tools to pediatric physician practice groups, is providing notice that an unauthorized third party was able to gain access to an internal computer network. The live electronic medical record was not accessed and the incident did not affect any pediatric practice groups' systems, databases, or medical records system at all.

On August 26, 2022, Connexin detected a data anomaly on our internal network. We immediately launched an investigation and engaged third-party forensic experts to determine the nature and scope of the incident. On September 13, 2022, we learned that an unauthorized party was able to access an offline set of patient data used for data conversion and troubleshooting. Some of that data was removed by the unauthorized party. The live electronic record system was not accessed in this incident, and the incident did not involve any physician practice group's systems, databases, or medical records system at all. Connexin is not aware of any actual or attempted misuse of personal information as a result of this event.

The patient information may have included: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider). Please note that not all data fields may have been involved for all individuals. Information of a parent, guardian, or guarantor may also have been impacted by the incident.

Data security is very important to us. As soon as we discovered the incident, we immediately took action to stop the unauthorized activity. This included a password reset of all corporate accounts and moving all patient data used for data conversion and troubleshooting into an environment with even greater security. Connexin also retained a third-party cybersecurity forensic firm to investigate the issue and is working with law enforcement to investigate the incident. In response to this incident, Connexin has enhanced its security and monitoring as well as further hardened its systems as appropriate to minimize the risk of any similar incident in the future.

The enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your child's personal information. We encourage you to carefully review credit reports and statements sent from providers as well as your insurance company to ensure that all account activity is valid; any questionable charges should be promptly reported to the provider's billing office, or for insurance statements, to your insurance company.

If your child's SSN was impacted, Connexin has arranged to offer your child identity monitoring services for a period of one year, at no cost to you, through Kroll (our third party vendor). You have 6 months from the date of your notice letter to activate these services, and instructions on how to activate these services are included in your notice letter.

Individuals who may have been impacted by this event are being mailed notices. Since it is possible there may be insufficient or out-of-date contact information for some individuals whose information was impacted, this notice is also accessible via Connexin's website at https://www.officepracticum.com/substitute-notice/ and the affected physician practice groups' websites, consistent with HIPAA.

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, or call toll-free 855-532-0912. This call center is open from 8:00am – 5:30pm CT, Monday through Friday, excluding some U.S. holidays.

We sincerely regret and apologize that this incident occurred. Connexin takes the security of personal information seriously, and we will continue to work diligently to protect the information entrusted to us.

This notice is being provided on behalf of the following physician practices/practice groups:

ABC Pediatrics Practice, PC

Academy Pediatrics, PA

Advanced Care Pediatric Centre, PLLC

Alice Tanner, M.D., PC

All Star Pediatrics, LLC

Angel Kids Pediatrics

Arlington Pediatric Partners, PLLC d/b/a Kids Docs Pediatrics

Kidswood Pediatrics, Inc.

Kidzcare Pediatrics, PC

KION Pediatrics, PLLC

Madison Pediatric Associates, PC

Maria Luisa Lira, M.D., PA

Mariano D. Cibran, M.D., Inc. d/b/a St. Petersburg Pediatrics

Maryland Pediatric Care, LLC

Ascension Medical Group f/k/a Pediatric Associates, PA

August Pediatrics, PA

Austex Pediatrics, PA

Bristow Pediatrics, PLLC

Burlington Pediatrics, PA

Carolina Pediatrics and Adolescent Care, PA

Casey Thomas Mulcihy Austin Texas, PA

Central Coast Pediatrics, Inc.

Children's Clinic, Ltd.

Children's Health Center of Columbus, Inc.

Children's Mercy – Pediatric Partners, Inc.

Children's Mercy – Shawnee Mission Pediatrics

Children's Pediatric Center Northside, LLC

Community Pediatrics, SC

Crockett Kids Pediatrics, PC

Dr. Michael J Ulich Pediatrics, LLC

Drexel Hill Pediatric Associates, PC

Eastern Carolina Pediatrics, PA

Eastern Shore Children's Clinic, PC

Ekta Khurana, M.D., PLLC

Maryvale Pediatric Specialists, LLC

Mayura Madani, M.D., PLLC

McComb Children's Clinic, Ltd.

Northeast Pediatric Night Clinic, Inc.

Oregon City Pediatrics

Orland Children's Center, Inc.

Passaic Pediatrics II, PA

Pensacola Pediatrics PA

Pediatric Associates of Lawrenceville, LLC

Pediatric Care Center No. 2, Inc.

Pediatric Center for Wellness, PC

Pediatric Health Center of El Paso

Pediatric Healthcare Associates of McKinney

Pediatric MultiCare West, LLC

Pediatric Physicians of Reston, PC

Pediatrics East, PC

Peds First Pediatrics

Petoskey Pediatrics PC

Phillips Pediatrics, PC

Premiere Pediatrics, PLLC

QC Kidz Pediatrics, PLLC

Rachel Z. Chatters, M.D., Inc

Raleigh Group, PC

Emily B. Vigour, M.D., LLC d/b/a Vigour Pediatrics

Ennis Pediatric and Adolescent Health Care, PA

Forest Hill Pediatrics, LLC MD

Fox Pediatrics, PLLC

Fraser-Branche Medical, PLLC

Gaurang Patel, M.D., LLC

Gold Pediatrics, PA

Goldsboro Pediatrics, PA

Goodlettsville Pediatrics, PC

Graham Pediatrics of Woodstock, LLC

Great Bend Children's Clinic, PA

Hatboro Pediatrics, PC

Hawthorne Pediatrics, LLC

Hebron Pediatrics, LLC

Helena Pediatric Clinic, PC

Holmdel Pediatrics, LLC

Honeygo Pediatrics, LLC

Jackson Pediatric Associates, PA

Jaleh Niazi, M.D., PC d/b/a New Day Pediatrics

James A. Weidman, AMC

Jose F. Alvarado & Associates, PA

Kerrville Pediatrics, PLLC

Kids First Pediatric Care, PA

Rankin Children's Group, PLLC

Raza Ali, MD, PC

Reading Pediatrics, Inc.

Renaissance Pediatrics, P.C.

Ruth Agwuna, M.D.

Samuel R Williams, M.D., PA

San Marino Pediatric Associates

SchoolCare, Inc. f/k/a CareDox, Inc.

SCS LLC d/b/a Bayshore Pediatrics

Sistema Infantil Teleton USA, Inc. a/k/a CRITS

South River Pediatrics, LLC

Springfield Medical, LLC

Sumter Pediatrics, LLC

Texoma Pediatrics, PLLC

The Pediatric & Adolescent Clinic, Inc.

The Pediatric Center of Frederick, LLC

Thomasville-Archedale Pediatrics, PLLC

Thompson River Pediatrics and Urgent Care, LLC

Valley Children's Medical Group

Virginia Pediatric Group, Ltd.

Watch Us Grow Pediatrics, PC

We Care Pediatrics, PC

Winsted Pediatrics

Kids Kare Pediatrics, PLLC

Yazji Pediatrics

Kids World Pediatrics, LLC

Zero Pediatrics, PLLC

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide any updated personal information to your health care provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the

credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Activate Kroll Identity Monitoring Services

As a safeguard, we have arranged for you to activate, at no cost to you, in online identity monitoring services provided by Kroll.

To activate this service, please the instructions for activation in your notice letter.

The monitoring included in the membership must be activated to be effective. You have until 6 months from the date of your notice letter to activate these services. Please note that identity monitoring services may not be available for individuals who do not have an address in the United States (or its territories) and a valid Social Security number. Activating this service will not affect your credit score.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission

Consumer Response Center

600 Pennsylvania Avenue, NW

Washington, DC 20580

1-877-IDTHEFT (438-4338)

www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	888-298-0045	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of the District of Columbia

You may contact the D.C. Attorney General's Office to obtain information about steps to take to avoid identity theft:

D.C. Attorney General's Office, Office of Consumer Protection, 400 6th Street, NW, Washington DC 20001, 1-202-442-9828, www.oag.dc.gov.

For Residents of Iowa

You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at:

Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowattorneygeneral.gov.

For Residents of Maryland

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, http://www.marylandattorneygeneral.gov/.

For Residents of Massachusetts

You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Residents of New Mexico

New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your

credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For Residents of New York

You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, www.ncdoj.gov.

For Residents of Oregon

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us.

For Residents of Rhode Island

You have a right to file or obtain a police report related to this incident. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Office of the Attorney General, 150 South Main Street, Providence, RI, 02903, 1-401-274-4400, www.riag.ri.gov.